TUGAS JARINGAN KOMPUTER

Analisis Paket Data dengan Mengunakan Wireshark dan Command Prompt

Nama : Endi Kumara

NIM : 09011281520098

Kelas : SK5 C

Dosen Pengampuh : Deris Stiawan, M.T., Ph.D

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

I. Pengertian Wireshark

Wireshark merupakan salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya terrmasuk protokol didalamnya. Wireshark banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis. Wireshark mampu menangkap paket-paket data atau informasi yang berseliweran dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang tool ini juga dapat dipakai untuk sniffing (memperoleh informasi penting spt password email atau account lain) dengan menangkap paket-paket yang berseliweran di dalam jaringan dan menganalisanya. Wireshark dipakai oleh network administrator untuk menganalisa kinerja jaringannya. Wireshark mampu menangkap paket-paket data atau informasi yang berjalan dalam jaringan yang terlihat dan semua jenis informasi ini dapat dengan mudah dianalisa yaitu dengan memakai sniffing , dengan sniffing diperoleh informasi penting seperti password email account lain. Wireshark merupakan software untuk melakukan analisa lalu-lintas jaringan komputer, yang memiliki fungsi-fungsi yang amat berguna bagi profesional jaringan, administrator jaringan, peneliti, hingga pengembang piranti lunak jaringan.

II. Pengertian Command Prompt (CMD)

CMD (Command Prompt) adalah sebuah perintah dos yang terdapat pada Windows yang bisa memudahkan pengguna dalam menjelajahi windows secara online maupun offline.

III. Tabel IP Source dan IP Destinatiion

- www.kompas.com

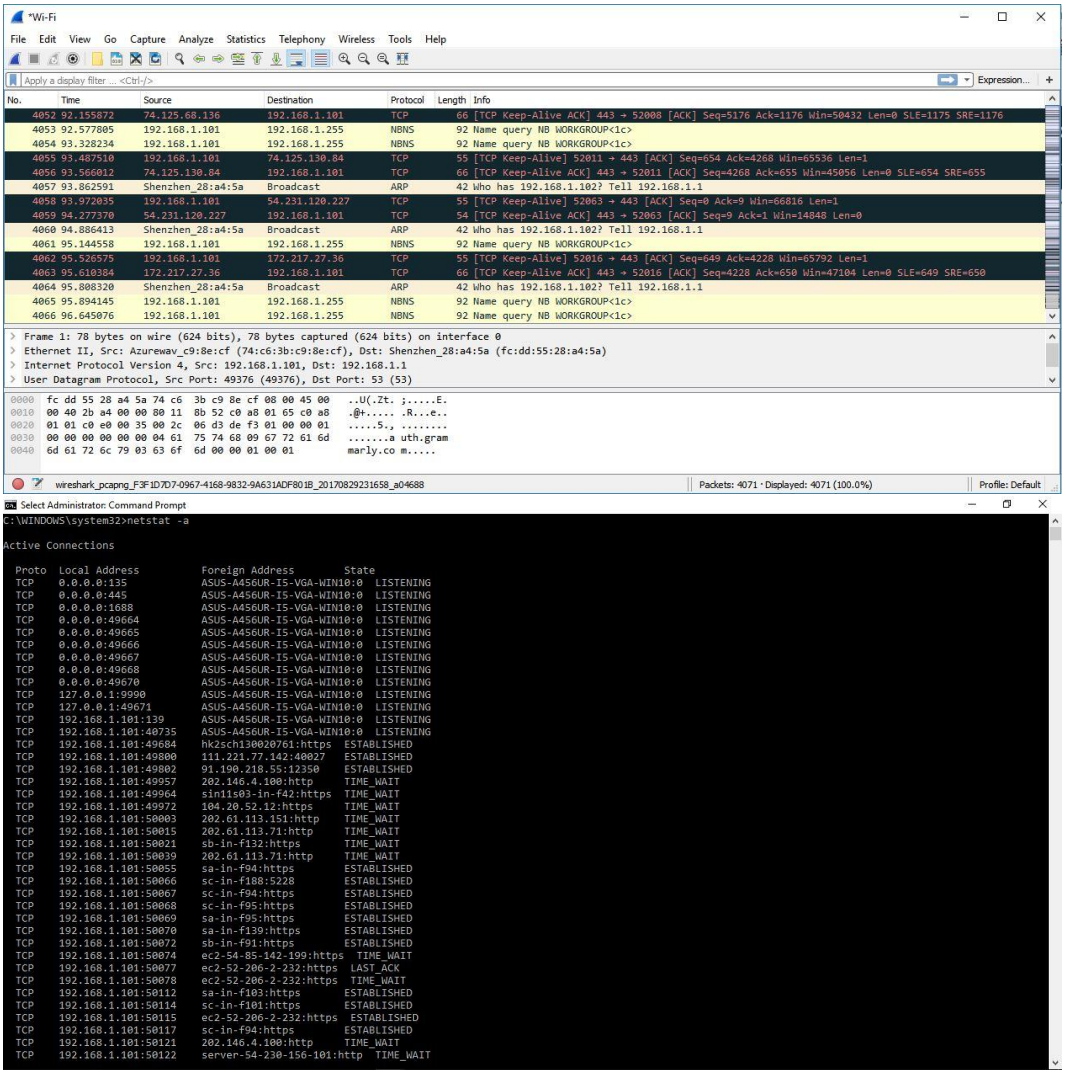
TABEL (www.kompas.com)		
Source		
IP Source	IP Destination	
192.168.1.101	202.146.4.100	[TCP Keep-Alive] 49957 → 80 [ACK] Seq=383 Ack=21679 Win=64860 Len=1
192.168.1.101	202.146.4.100	49957 → 80 [ACK] Seq=384 Ack=12741 Win=64860 Len=0
192.168.1.101	202.146.4.100	[TCP Dup ACK 1369#1] 49957 → 80 [ACK] Seq=384 Ack=1 Win=64240 Len=0 SLE=1381 SRE=2761
192.168.1.101	202.146.4.100	49957 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.1.101	202.146.4.100	49957 → 80 [ACK] Seq=384 Ack=2761 Win=64860 Len=0
Destination		
IP Source	IP Destination	
202.146.4.100	192.168.1.101	[TCP Keep-Alive ACK] 80 → 49957 [ACK] Seq=21679 Ack=384 Win=4523 Len=0
202.146.4.100	192.168.1.101	80 → 49957 [ACK] Seq=12741 Ack=384 Win=4523 Len=1380
202.146.4.100	192.168.1.101	[TCP Out-Of-Order] 80 → 49957 [ACK] Seq=1 Ack=384 Win=4523 Len=1380
202.146.4.100	192.168.1.101	80 → 49957 [ACK] Seq=1 Ack=384 Win=4523 Len=0
202.146.4.100	192.168.1.101	80 → 49957 [PSH, ACK] Seq=2761 Ack=384 Win=4523 Len=320

- www.lk21.net

A	B	C	D
TABEL (lk21.net)			
Source			
IP Source	IP Destination		
192.168.1.101	104.31.72.126	52307 → 80 [ACK] Seq=504 Ack=8365 Win=66816 Len=0 SLE=13941 SRE=15335	
192.168.1.101	104.31.72.127	52307 → 80 [ACK] Seq=504 Ack=9759 Win=66816 Len=0 SLE=11153 SRE=12547 SLE=13941 SRE=15335	
192.168.1.101	104.31.72.128	52307 → 80 [ACK] Seq=504 Ack=12547 Win=66816 Len=0 SLE=13941 SRE=15335	
192.168.1.101	104.31.72.129	52307 → 80 [ACK] Seq=504 Ack=15335 Win=66816 Len=0	
192.168.1.101	104.31.72.130	[TCP Dup ACK 733#1] 52307 → 80 [ACK] Seq=504 Ack=15335 Win=66816 Len=0 SLE=16729 SRE=18123	
Destination			
IP Source	IP Destination		
104.31.72.126	192.168.1.101	[TCP Retransmission] 80 → 52307 [ACK] Seq=11153 Ack=504 Win=30720 Len=1394	
104.31.72.127	192.168.1.101	[TCP Retransmission] 80 → 52307 [ACK] Seq=9759 Ack=504 Win=30720 Len=1394	
104.31.72.128	192.168.1.101	[TCP Retransmission] 80 → 52307 [ACK] Seq=12547 Ack=504 Win=30720 Len=1394	
104.31.72.129	192.168.1.101	[TCP Previous segment not captured] 80 → 52307 [ACK] Seq=16729 Ack=504 Win=30720 Len=1394	
104.31.72.130	192.168.1.101	80 → 52307 [ACK] Seq=18123 Ack=504 Win=30720 Len=1394	

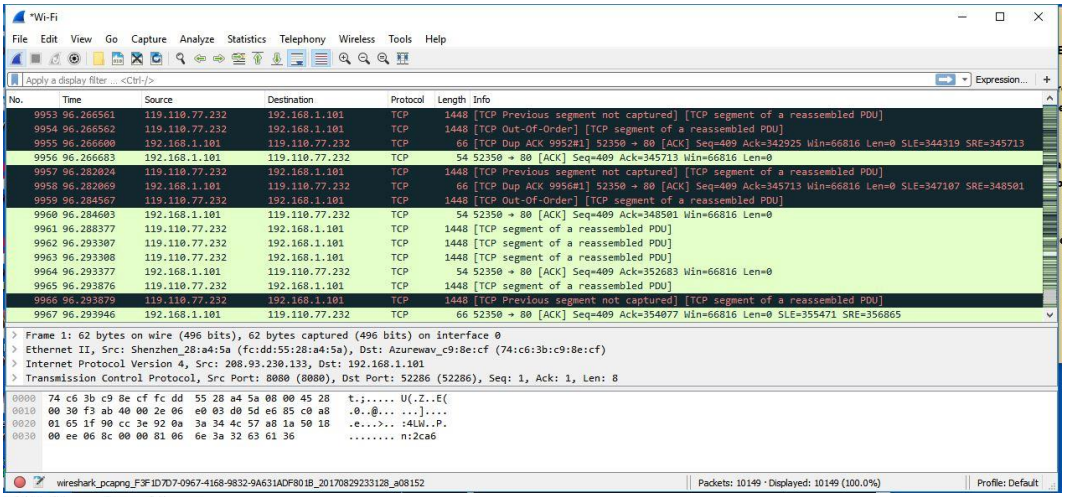
IV. Analisis Wireshark dan Command Prompt

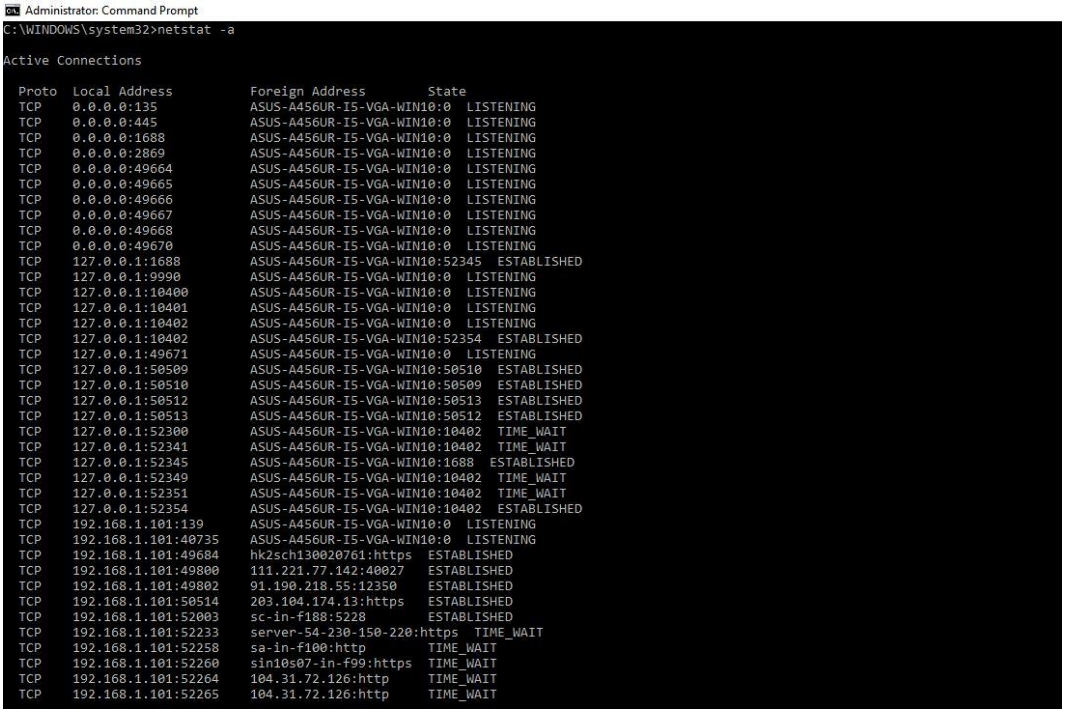
- ❖ www.kompas.com



Analisis: setelah melihat data dari wireshark dan command prompt terlihat pada wireshark lebih detail dalam memberikan info paket data yg berupa ip source, ip destination, protocol, length, info, time, dan nomor. Sedangkan pada CMD hanya berupa protocol, ip source, address, dan state. Dengan menggunakan wireshark kita bisa mengetahui info yang terdapat di dalam paket data tersebut.

- www.lk21.net





Analisis: Untuk yang streaming bisa di lihat bahwa paket data lebih banyak dari pada paket data pada kompas.com tadi. Dan pada CMD nya juga lebih banyak dari pada kompas.com. hal ini mungkin di sebabkan karena pada saat streaming membutuh kan bandwith yang besar.